### Security Extension for OSPFv2 when using Manual Key Management
#### draft-ietf-ospf-security-extension-manual-keying-00

Abstract

   The current OSPFv2 cryptographic authentication mechanism as defined
   in the OSPF standards is vulnerable to both inter-session and intra-
   session replay attacks when its uses manual keying.  Additionally,
   the existing cryptographic authentication schemes do not cover the IP
   header.  This omission can be exploited to carry out various types of
   attacks.

   This draft proposes changes to the authentication sequence number
   mechanism that will protect OSPFv2 from both inter-session and intra-
   session replay attacks when its using manual keys for securing its
   protocol packets.  Additionally, we also describe some changes in the
   cryptographic hash computation so that we eliminate most attacks that
   result because OSPFv2 does not protect the IP header.

Status of this Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF).  Note that other groups may also distribute
   working documents as Internet-Drafts.  The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time.  It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on November 7, 2011.

Copyright Notice

Table of Contents

## 1.  Introduction

The OSPFv2 cryptographic authentication mechanism as described in
[[RFC2328]] uses per-packet sequence numbers to provide protection
against replay attacks.  The sequence numbers increase monotonically
so that the attempts to replay the stale packets can be thwarted.
The sequence number values are maintained as a part of adjacency
states.  Therefore, if an adjacency is broken down, the associated
sequence numbers get reinitialized and the neighbors start all over
again.  Additionally, the cryptographic authentication mechanism does
not specify how to deal with the rollover of a sequence number when
its value would wrap.  These omissions can be taken advantage of by
attackers to implement various replay attacks ([RFC6039]).  In order
to address these issues, we propose extensions to the authentication
sequence number mechanism.  Compared with the cryptographic
authentication mechanism proposed in [RFC5709], the solution proposed
does not impose any more security presumption.

The cryptographic authentication as described in [RFC2328] and later
updated in [RFC5709] does not include the IP header.  This also can
be exploited to launch several attacks as the source address in the
IP header is no longer protected.  The OSPF specification, for
broadcast and NBMA (Non-Broadcast Multi-Access Networks), requires
the implementations to look at the source address in the IP header to
determine the neighbor from witch the packet was received.  Changing
the IP source address of a packet which can confuse the receiver and
can be exploited to produce a number of denial of service attacks
[RFC6039].  If the packet is interpreted as coming from a different
neighbor, the sequence number received from the neighbor may be
updated.  This may disrupt communication with the legitimate
neighbor.  Hello packets may be reflected to cause a neighbor to
appear to have one-way communication.  Old Database descriptions may
be reflected in cases where the per-packet sequence numbers are
sufficiently divergent in order to disrupt an adjacency
[I-D.ietf-karp-ospf-analysis].  This is referred to as the IP layer
issue in [I-D.ietf-karp-threats-reqs].

[RFC2328] states that implementations MUST offer keyed MD5
authentication.  It is likely that this will be deprecated in favor
of the stronger algorithms described in [RFC5709] in future
deployments [I-D.ietf-opsec-igp-crypto-requirements].

This draft proposes a simple change in the cryptographic
authentication mechanism, as currently described in [RFC5709], to
prevent such IP layer attacks.

## 1.1.  Requirements Section

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

When used in lowercase, these words convey their typical use in common language, and are not to be interpreted as described in RFC2119 [RFC2119].

## 2.  Replay Protection using Extended Sequence Numbers

In order to provide replay protection against both inter-session and intra-session replay attacks, the OSPFv2 sequence number is expanded to 64-bits with the least significant 32-bit value containing a strictly increasing sequence number and the most significant 32-bit value containing the boot count.  OSPFv2 implementations are required to retain the boot count in non-volatile storage for the deployment life the OSPF router.  The requirement to preserve the boot count is also placed on SNMP agents by the SNMPv3 security architecture (refer to snmpEngineBoots in [RFC4222].

Since there is no room in the OSPFv2 packet for a 64-bit sequence number, it will occupy the 8 octets following the OSPFv2 packet and MUST be included when calculating the OSPFv2 packet digest.  These additional 8 bytes are not included in the OSPFv2 packet header length but are included in the OSPFv2 header Authentication Data length and the IPv4 packet header length.

The lower order 32-bit sequence number MUST be incremented for every OSPF packet sent by the OSPF router.  Upon reception, the sequence number MUST be greater than the sequence number in the last OSPF packet of that type accepted from the sending OSPF neighbor. Otherwise, the OSPF packet is considered a replayed packet and dropped.  OSPF packets of different types may arrive out of order if they are priorized as recommended in [RFC3414].

OSPF routers implementing this specification MUST use available mechanisms to preserve the sequence number's strictly increasing property for the deployed life of the OSPFv3 router (including cold restarts).  This is achieved by maintaining a boot count in non-volatile storage and incrementing it each time the OSPF router loses its prior sequence number state.  The SNMPv3 snmpEngineBoots variable [RFC4222] MAY be used for this purpose.  However, maintaining a separate boot count solely for OSPF sequence numbers has the advantage of decoupling SNMP reinitialization and OSPF reinitialization.  Also, in the rare event that the lower order 32-

bit sequence number wraps, the boot count can be incremented to
preserve the strictly increasing property of the aggregate sequence
number.  Hence, a separate OSPF boot count is RECOMMENDED.


3.  OSPF Packet Extensions

The OSPF packet header includes an authentication type field, and 64-
bits of data for use by the appropriate authentication scheme
(determined by the type field).  Authentication types 0, 1 and 2 are
defined [RFC2328].  This section of this defines Authentication type
TBD (3 is recommended).

When using this authentication scheme, the 64-bit Authentication
field in the OSPF packet header as defined in section D.3 of
[RFC2328] is changed as shown below.  The sequence number is removed
and the Key ID is extended to 32 bits and moved to the former
position of the sequence number.

Additionally, the 64-bit sequence number is moved to the first 64-
bits following the OSPFv2 packet and is protected by the
authentication digest.  These additional 64 bits or 8 octets are
included in the IP header length but not the OSPF header packet
length.

```
        0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       | Version # |     Type      |         Packet length           |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                          Router ID                           |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                          Area ID                             |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |         Checksum          |               AuType             |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                           0                   | Auth Data Len |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                           Key ID                             |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                              |
       |                     OSPF Protocol Packet                     |
       ~                                                              ~
       |                                                              |
       |                                                              |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |      Sequence Number (Boot Count)                            |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |      Sequence Number (Strictly Increasing Packet Counter)    |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                              |
       ~                      Authentication Data                     ~
       |                                                              |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

        Figure 7 -  Extended Sequence Number Packet Extensions

## 4.  OSPF Packet Key Selection

   This section describes how the proposed security solution selects
   long-lived keys from key tables.  [I-D.ietf-karp-crypto-key-table].
   Generally, a key used for OSPFv2 packet authentication should satisfy
   the following requirements:

   o  The key time period as defined by NotBefore and NotAfter must
      include the current time.

   o  The key can be used for the desired security algorithm.

   In the remainder of this section, additional requirements for keys
   are enumerated for different scenarios.

## 4.1.  Key Selection for Unicast OSPF Packet Transmission

   Assume that a router R1 tries to send a unicast OSPF packet from its
   interface I1 to the interface R2 of a remote router R2 using security
   protocol P via interface I at time T. Firstly consider the
   circumstances where R1 and R2 are not connected with a virtual link.
   R1 then needs to select a long long-lived symmetric key from its key
   table.  Because the key should be shared by the by both R1 and R2 to
   protect the communication between I1 and I2, the key should satisfy
   the following requirements:

   o  The Peer field includes the router ID of R2.

   o  the PeerKeyID field is not "unknown".

   o  The Interfaces field includes I1.

   o  the Direction field is either "out" or "both".

   When R1 and R2 are connected to a virtual link, the third condition
   is a little more complex.  Because the virtual link can be regarded
   as an unnumbered point-to-point network, the IP address of the
   interface actually used to send the packet (i.e., I1) is discovered
   during routing table calculation.  Therefore, when the system
   operator configures keys to protect the virtual link, I1 is unknown
   and can be any OSPF interface in the OSPF virtual link's transit
   area.  Therefore, the key should be identified solely by the local
   and remote router IDs rather than by the interface on which the
   packet is sent.  The third requirement list above should be changed
   to "the Interface field includes the router ID".

## 4.2.  Key Selection for Multicast OSPF Packet Transmission

   If a router R1 sends an OSPF packet from its interface I1 to a
   multicast address (e.g., AllSPFRouters, AllDRouters), it needs to
   select a key according to the following requirements:

   o  The Peer field includes the multicast address.

   o  The PeerKeyID field is "group".

   o  The Interfaces field includes I1.

   o  The Direction field is either "out" or "both".

### 4.3.  Key Selection for OSPF Packet Reception

When Cryptographic Authentication is employed, the ID of the
authentication key is included in the authentication field of the
OSPF packet header.  Using this key ID, it is relatively easy for a
receiver to locate the key.  The simple requirements are:

o  The Peer field includes the router ID of the sender.

o  The PeerKeyID field includes the key ID obtained from the
   authentication field.

o  The Direction field is either "in" or "both".


### 5.  Mechanism to secure the IP header

This document updates the definition of Apad which is currently a
constant defined in [RFC5709] to the source address from the IP
header of the OSPFv2 protocol packet.  The overall cryptographic
authentication process defined in [RFC5709] remains unchanged.  To
reduce the potential for confusion, this section minimizes the
repetition of text from RFC 5709 and is incorporated here by
reference [RFC5709].

RFC 5709, Section 3.3, describes how the cryptographic authentication
must be computed.  It requires OSPFv2 packet's Authentication Trailer
(which is the appendage described in RFC 2328, Section D.4.3, Page
233, items (6)(a) and (6)(d)) to be filled with the value Apad where
Apad is a hexadecimal constant value 0x878FE1F3 repeated (L/4) times,
where L is the length of the hash being used and is measured in
octets rather than bits.

Routers at the sending side must initialize Apad to a value of the
source address that would be used when sending out the OSPFv2 packet,
repeated L/4 times, where L is the length of the hash, measured in
octets.  The basic idea is to incorporate the source address from the
IP header in the cryptographic authentication computation so that any
change of IP source address in a replayed packet can be detected.

At the receiving end, implementations MUST initialize Apad as the
source address from IP Header of the incoming OSPFv2 packet, repeated
L/4 times, instead of the constant that's currently defined in
[RFC5709].  Besides changing the value of Apad, this document does
not introduce any other changes to the authentication mechanism
described in [RFC5709].  This would prevent all attacks where a rogue
OSPF router changes the IP source address of an OSPFv2 packet and
replays it on the same multi-access interface or another interface

    since the IP source address is now protected and such changes would
    cause the authentication check to fail and the replayed packet to be
    rejected.


6.  Security Considerations

    This document attempts to fix the manual key management procedure
    that currently exists within OSPFv2, as part of the Phase 1 of the
    KARP Working Group.  Therefore, only the OSPFv2 manual key management
    mechanism is considered.  Any solution that takes advantage of the
    automatic key management mechanism is beyond the scope of this
    document.

    The proposed sequence number extension offers most of the benefits of
    of more complicated mechanisms involving challenges.  There are,
    however, a couple drawbacks to this approach.  First, it requires the
    OSPF implementation to be able to save its boot count in non-volatile
    storage.  If the non-volatile storage is ever repaired or upgraded
    such that the contents are lost or the OSPFv2 router is replaced with
    a model, the keys MUST be changed to prevent replay attacks.

    Second, if a router is taken out of service completely (either
    intentionally or due to a persistent failure), the potential exists
    for reestablishment of an OSPFv2 adjacency by replaying the entire
    OSPFv2 session establishment.  This scenario is however, extremely
    unlikely, since it would imply an identical OSPFv2 adjacency
    formation packet exchange.  The replay of OSPFv2 hello packets alone
    for an OSPFv2 router that has been taken out of service should not
    result in any serious attack as the only consequence is superfluous
    processing.  Of course, this attack could also be thwarted by
    changing the relevant manual keys.

    This document also provides a solution to prevent certain denial of
    service attacks that can be launched by changing the source address
    in the IP header of the OSPFv2 protocol packet.


7.  IANA Considerations

    This document requests a new code point from the "OSPF Shortest Path
    First (OSPF) Authentication Codes" registry:

    o  TBD - Cryptographic Authentication with Extended Sequence Numbers.
       The value 3 is recommended.


8.  References

### 8.1.  Normative References

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2328]   Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC5709]   Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M.,
            Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic
            Authentication", RFC 5709, October 2009.

### 8.2.  Informative References

[I-D.ietf-karp-crypto-key-table]
            Housley, R. and T. Polk, "Database of Long-Lived Symmetric
            Cryptographic Keys", draft-ietf-karp-crypto-key-table-00
            (work in progress), November 2010.

[I-D.ietf-karp-ospf-analysis]
            Hartman, S. and D. Zhang, "Analysis of OSPF Security
            According to KARP Design Guide",
            draft-ietf-karp-ospf-analysis-00 (work in progress),
            March 2011.

[I-D.ietf-karp-threats-reqs]
            Lebovitz, G., Bhatia, M., and R. White, "The Threat
            Analysis and Requirements for Cryptographic Authentication
            of Routing Protocols' Transports",
            draft-ietf-karp-threats-reqs-02 (work in progress),
            April 2011.

[I-D.ietf-opsec-igp-crypto-requirements]
            Bhatia, M. and V. Manral, "Summary of Cryptographic
            Authentication Algorithm Implementation Requirements for
            Routing Protocols",
            draft-ietf-opsec-igp-crypto-requirements-04 (work in
            progress), October 2010.

[RFC3414]   Blumenthal, U. and B. Wijnen, "User-based Security Model
            (USM) for version 3 of the Simple Network Management
            Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[RFC4222]   Choudhury, G., "Prioritized Treatment of Specific OSPF
            Version 2 Packets and Congestion Avoidance", BCP 112,
            RFC 4222, October 2005.

[RFC6039]   Manral, V., Bhatia, M., Jaeggli, J., and R. White, "Issues
            with Existing Cryptographic Protection Methods for Routing

                  Protocols", RFC 6039, October 2010.


Authors' Addresses

   Manav Bhatia
   Alcatel-Lucent
   Bangalore,
   India

   Phone:
   Email: manav.bhatia@alcatel-lucent.com


   Sam Hartman
   Painless Security

   Email: hartmans@painless-security.com


   Dacheng Zhang
   Huawei Technologies co., LTD.
   Beijing,
   China

   Phone:
   Fax:
   Email: zhangdacheng@huawei.com
   URI:


   Acee Lindem
   Ericsson
   102 Carric Bend Court
   Cary,   NC 27519
   USA

   Phone:
   Email: acee.lindem@ericsson.com